



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/702,167	11/05/2003	Nancy Cam Winget	72255/00006	7272
23380	7590	05/18/2007	EXAMINER	
TUCKER, ELLIS & WEST LLP 1150 HUNTINGTON BUILDING 925 EUCLID AVENUE CLEVELAND, OH 44115-1414			DEBNATH, SUMAN	
ART UNIT		PAPER NUMBER		
		2135		
MAIL DATE		DELIVERY MODE		
05/18/2007		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)
	10/702,167	WINGET ET AL.
	Examiner	Art Unit
	Suman Debnath	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
 - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
 - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 03/05/2007.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-27 is/are pending in the application.
 - 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-27 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date: _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date: _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-27 are pending in this application and presented for examination.
2. Claims 1, 9 and 17 are presently amended.
3. Claims 25-27 have been newly presented in the amendment filed on March 5th 2007.

Claim Objections

4. Claims 1 and 9 are objected to for lack of antecedent basis:
Claim 1 recites "the at least first and second parties" in line 3.
Claim 9 recites "the at least first and second parties" in line 3.
Appropriate correction is required.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1-24 are rejected under 35 U.S.C. 102(b) as being anticipated by Funk (Paul Funk; Simon Blake-Wilson; "draft-ietf-pppext-eap-ttls-02.txt: EAP Tunneled TLS Authentication Protocol (EAP-TTLS)"; Internet-Draft PPPEXT Working Group; Nov. 2002, p. 1-40).

7. As to claim 1, Funk discloses a method of secure communication comprising: establishing a secure tunnel between the at least first and second parties using an encryption algorithm that establishes an encryption key (Pages 9-10, section 4.3; Pages 11-13, sections 6-6.2,); authenticating with an authentication server over the secured tunnel establishing an authentication key (Pages 9-10, section 4.3; Pages 11-13, sections 6-6.2 and Page 20, section 10); verifying by the first party that the second party possess the same encryption and authentication keys as the first party (Pages 9-10, section 4.3; Pages 11-13, sections 6-6.2; and Page 20, section 10), and; provisioning secure credentials between the at least first and second parties using the secured tunnel, responsive to the verifying the second party possess the same encryption and authentication keys as the first party (Pages 9-10, section 4.3; Pages 11-16, section 6-7, Page 20, section 10).

8. As to claim 9 and 17, these are rejected using the same rationale as for the rejection of claim 1.

9. As to claims 2, 10 and 18, Funk discloses wherein the communication implementation between the at least first and second parties is at least one of a wired implementation and a wireless implementation (Pages 4-5, section 2).

10. As to claims 3, 11 and 19, Funk discloses wherein the encryption algorithm is an asymmetric encryption algorithm (Page 9-10; sections 4.2-4.3; Page 28, section 12).

11. As to claims 4, 12 and 20, Funk discloses wherein the asymmetric encryption algorithm is used to derive a shared secret, subsequently used in the step of establishing a secure tunnel (Page 9-10; sections 4.2-4.3; Page 28, section 12).
12. As to claims 5, 13 and 21, Funk discloses wherein the asymmetric encryption algorithm is Diffie-Hellman key exchange (Pages 36-37, section 14).
13. As to claims 6, 14 and 22, Funk discloses wherein the step of authenticating is performed using Microsoft MS-CHAP v2 (Pages 11-12; section 6; Pages 23-24, section 10.2.4).
14. As to claims 7, 15 and 23, Funk discloses further comprising a step of provisioning a public/private key pair on one of the at least first and second parties, and then to provision that public key on the respective remaining ones of the at least first and second parties (Pages 11-16, sections 6-7).
15. As to claims 8, 16 and 24, Funk discloses wherein the step of provisioning a public/private key pair comprises providing a server-side certificate in accordance with Public Key Infrastructure (PKI) (Pages 9-10, sections 4.2-4.3, Page 20, section 10).

Claim Rejections - 35 USC § 103

16. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

17. Claims 25-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Funk and further in view of Palekar et al. (Pub. No.: US 2003/0226017 A1), hereinafter "Palekar".

18. As to claims 25, 26 and 27, Funk doesn't explicitly disclose wherein the verifying further comprises hashing the first party encryption key and the authentication key to produce a first hash; hashing the second party encryption key and the second party authentication key to produce a second hash; verifying the first and second hash are the same. However, Palekar discloses wherein the verifying further comprises hashing the first party encryption key and the authentication key to produce a first hash; hashing the second party encryption key and the second party authentication key to produce a second hash; verifying the first and second hash are the same ([0008], [0044], [0079]).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Funk as taught by Palekar in order to increase the confidentiality and integrity of the data that transmit over the public network.

Response to Argument

19. Applicant has amended claims 1, 9 and 17 and newly presented claims 25-27 which necessitated new ground of rejections. See rejection above.

Conclusion

20. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See accompanying PTO 892.

US 2004/0034772 A1 – Method and system for accelerated data encryption.

21. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Art Unit: 2135

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Suman Debnath whose telephone number is 571 270 1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SD

H/T S
HOSUK SONG
PRIMARY EXAMINER